U3-03082-KS

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年　９月１７日

出願番号
Application Number: 特願２００２－２７０５４３

[ST.10/C]: [ＪＰ２００２－２７０５４３]

出願人
Applicant(s): 株式会社デンソー

２００３年　７月　４日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３０５３２４４

【書類名】　特許願
【整理番号】　PSN405
【提出日】　平成14年 9月17日
【あて先】　特許庁長官殿
【国際特許分類】　E05B 49/00
【発明者】
　【住所又は居所】　愛知県刈谷市昭和町１丁目１番地　株式会社デンソー内
　【氏名】　辻　浩幸
【発明者】
　【住所又は居所】　愛知県刈谷市昭和町１丁目１番地　株式会社デンソー内
　【氏名】　奥村　亮三
【特許出願人】
　【識別番号】　000004260
　【氏名又は名称】　株式会社デンソー
【代理人】
　【識別番号】　100106149
　【弁理士】
　【氏名又は名称】　矢作　和行
　【電話番号】　052-220-1100
【手数料の表示】
　【予納台帳番号】　010331
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　遠隔操作装置

【特許請求の範囲】

【請求項１】　装置毎に固有に定められた固有キーコードを用いて所定のコードを暗号化する暗号化手段を有し、この暗号化手段によって暗号化された暗号化コードを送信する送信機と、

前記暗号化コードを受信し前記固有キーコードを用いて前記暗号化コードを復号化する復号化手段を有し、この復号化手段によって復号化されたコードが記憶されているコードに対して所定の関係を満足しているときに、制御対象を作動させる指令を出力する受信機とを備える遠隔操作装置であって、

前記復号化手段が用いる前記固有キーコードを前記送信機から前記受信機へ送信して登録する場合、前記送信機は前記送信機及び前記受信機が記憶するデフォルトキーコードを用いて前記暗号化手段によって前記固有キーコードを暗号化したうえで前記受信機に対して送信することを特徴とする遠隔操作装置。

【請求項２】　前記送信機は、所定の操作がなされた場合に前記暗号化した固有キーコードを前記受信機に対して送信することを特徴とする請求項１記載の遠隔操作装置。

【請求項３】　装置毎に固有に定められた固有キーコードを用いて受信した所定のコードを暗号化する暗号化手段を有し、この暗号化手段によって暗号化された暗号化コードを送信する携帯機と、

前記携帯機に対して前記所定のコードを送信するとともに、その所定のコードに対して返送された前記暗号化コードを受信し前記固有キーコードを用いて前記暗号化コードを復号化する復号化手段を有し、この復号化手段によって復号化されたコードが送信したコードに対して所定の関係を満足しているときに、制御対象を作動させる指令を出力する車載制御機とを備える遠隔操作装置であって、

前記復号化手段が用いる前記固有キーコードを前記携帯機から前記車載制御機へ送信して登録する場合、前記携帯機は前記携帯機及び前記車載制御機が記憶するデフォルトキーコードを用いて前記暗号化手段によって前記固有キーコードを暗号化したうえで前記車載制御機に対して送信することを特徴とする遠隔操作装

置。

【請求項４】　前記携帯機は、所定の操作がなされた場合に前記暗号化した固有キーコードを前記車載制御機に対して送信することを特徴とする請求項３記載の遠隔操作装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、車両のワイヤレスドアロック制御等に用いられる遠隔操作装置に関するものである。

【０００２】

【従来の技術】

従来、車両のワイヤレスドアロック制御等に用いられる遠隔操作装置では、盗聴などの不正防止の観点から、送信機から送信する送信コードを暗号化して、ユーザによって解読されないように対策している。例えば、特許文献１に開示されている遠隔操作装置では、送信機が送信する毎に所定の順序で変更されるローリングコードを、装置毎に固有に定めたキーコードを用いて暗号化して暗号化ローリングコードを生成し、この暗号化ローリングコードを用いてＩＤコードをさらに暗号化している。そして、これらのコードを受信する受信機では、暗号化された暗号化ローリングコード及びＩＤコードを復元し、復元したＩＤコードが記憶しているＩＤコードに一致し、かつ、復元したローリングコードと記憶されるローリングコードとが所定の関係を満足している場合に、制御対象への指示信号を出力している。

【０００３】

このように、従来の遠隔操作装置では、ローリングコードを単に送信して照合するのではなく、キーコードという送信機と受信機とが共通して記憶するコードを用いてローリングコードを暗号化している。

【０００４】

【特許文献１】

特開平１０－６１２７７号公報

【０００５】

【発明が解決しようとする課題】

上述のローリングコードの暗号化に用いられるキーコードは、遠隔操作装置を製造する工程において、送信機から受信機に対してキーコードを送信し、受信機の不揮発性記憶媒体に記憶する。しかし、この従来の遠隔操作装置では、送信機から受信機へキーコードを送信する際、このキーコードを暗号化しない状態で送信機から送信していたため、この送信時にキーコードが盗聴される恐れがあった。そのため、キーコードによって暗号化されるローリングコードは、予め設定された順序で変更されるものであるため、例えば、この変更順序を設定した者（設計者）がキーコードを取得したならば、暗号化されたローリングコード及びＩＤコードの解読が可能となる。

【０００６】

本発明は、かかる問題を鑑みてなされたもので、受信機へキーコードを登録するときのキーコードの取得を防止することが可能な遠隔操作装置を提供することを目的とする。

【０００７】

【課題を解決するための手段】

請求項１に記載の遠隔操作装置は、装置毎に固有に定められた固有キーコードを用いて所定のコードを暗号化する暗号化手段を有し、この暗号化手段によって暗号化された暗号化コードを送信する送信機と、暗号化コードを受信し固有キーコードを用いて暗号化コードを復号化する復号化手段を有し、この復号化手段によって復号化されたコードが所定の関係を満足しているときに、制御対象を作動させる指令を出力する受信機とを備える遠隔操作装置であって、復号化手段が用いる固有キーコードを送信機から受信機へ送信して登録する場合、送信機は送信機及び受信機が記憶する所定の共通キーコードを用いて暗号化手段によって固有キーコードを暗号化したうえで受信機に対して送信することを特徴とする。

【０００８】

このように、例えば、車両のワイヤレスドアロック制御等に用いられる本発明の遠隔操作装置は、送信機の固有キーコードを暗号化したうえで受信機へ送信し

ている。これにより、送信機の固有キーコードを受信機へ送信して登録する際、固有キーコードが盗聴されたとしても、固有キーコードは暗号化されているため、固有キーコードの取得の困難性が向上できる。その結果、送信機の不正な複製を防止することが可能となる。

【０００９】

また、固有キーコードの暗号化は、制御対象を作動させるための所定のコードを暗号化する暗号化手段によって暗号化されるため、専用の暗号化アルゴリズムを用意する必要がなく、ソフト容量の節約や管理工数が削減できる。

【００１０】

請求項２に記載の遠隔操作装置によれば、送信機は、所定の操作がなされた場合に暗号化した固有キーコードを受信機に対して送信することを特徴とする。例えば、ユーザが通常することのない押しボタンの押し方、押す順序等を固有キーコードの登録に割り当てておくことで、固有キーコードを容易に受信機へ送信することが可能となる。

【００１１】

請求項３に記載の遠隔操作装置は、装置毎に固有に定められた固有キーコードを用いて受信した所定のコードを暗号化する暗号化手段を有し、この暗号化手段によって暗号化された暗号化コードを送信する携帯機と、携帯機に対して所定のコードを送信するとともに、その所定のコードに対して返送された暗号化コードを受信し固有キーコードを用いて暗号化コードを復号化する復号化手段を有し、この復号化手段によって復号化されたコードが所定の関係を満足しているときに、制御対象を作動させる指令を出力する車載制御機とを備える遠隔操作装置であって、復号化手段が用いる固有キーコードを携帯機から車載制御機へ送信して登録する場合、携帯機は携帯機及び車載制御機が記憶する所定の共通キーコードを用いて暗号化手段によって固有キーコードを暗号化したうえで車載制御機に対して送信することを特徴とする。

【００１２】

このように、携帯機と車載制御機との双方向通信によって、例えば、車両の各ドアのロック機構やステアリングロック機構を制御したり、車両のエンジンの始

動の許可・禁止状態を制御したりする電子キーシステムに、本発明の遠隔操作装置を適用することによって、固有キーコードの取得を困難なものとすることができる。その結果、携帯機の不正な複製を防止することが可能となる。

【００１３】

請求項４に記載の遠隔操作装置によれば、携帯機は、所定の操作がなされた場合に暗号化した固有キーコードを車載制御機に対して送信することを特徴とする。例えば、ユーザが通常することのない押しボタンの押し方、押す順序等を固有キーコードの登録に割り当てておくことで、固有キーコードを容易に受信機へ送信することが可能となる。

【００１４】

【発明の実施の形態】

以下、本発明の実施の形態における遠隔操作装置に関して、図面に基づいて説明する。

【００１５】

（第１の実施形態）

本実施形態では、本発明の遠隔操作装置を車両用のワイヤレスドアロック制御等を行う装置に採用した例について説明する。図１は、本実施形態の遠隔操作装置における、送信機１と受信機２の構成を示すブロック図である。

【００１６】

同図において、送信機１には、それぞれ異なった機能（例えば、車両の各ドアのロック・アンロック、トランクの開閉、シートポジションの設定等）を遠隔作動させるためのスイッチ１２－１、１２－２、・・・、１２－ｎが設けられており、そのスイッチ操作による信号がマイクロプロセッサ１１に入力するように構成されている。

【００１７】

このマイクロプロセッサ１１は、ＥＥＰＲＯＭ１３が接続されており、このＥＥＰＲＯＭ１３には、送信機固有のＩＤコード、送信機１が送信する毎に所定の順序で変化するローリングコード、車両固有のキーコード、及び登録用キーコード（デフォルトキーコード）が記憶されている。これらのＩＤコード、ローリン

グコード、キーコード、登録用キーコードは、車両の製造工程においてＥＥＰＲＯＭ１３に記憶されるものである。

【００１８】

また、ＥＰＰＲＯＭ１３には、マイクロプロセッサ１１がローリングコードを暗号化する際に用いる変更テーブル（図２）が記憶されるとともに、暗号化アルゴリズム（図３）がプログラムとして記憶されている。このプログラムに従って、マイクロプロセッサ１１にて暗号化処理が行われる。

【００１９】

図２に示すように、変更テーブルは、各々異なるｍビットからなるｎ個の共通鍵コード［ＫＥＹ（１）～ＫＥＹ（ｎ）］が設定されている。このうち、ｋ番目の共通鍵コードには、ＥＥＰＲＯＭ１３に記憶される車両固有のキーコードが設定されている。

【００２０】

さらに、マイクロプロセッサ１１には、発信回路１４及びＦＭ変調回路１５が接続されており、マイクロプロセッサ１１にて最終的に生成された送信コードを、ＦＭ変調したのち微弱電波として発信するように構成されている。

【００２１】

受信機２は、送信機１から発信された微弱電波を復調する受信回路が設けられている。この受信回路は、局部発振器２４、高周波増幅回路２５、ミキサ回路２６、中間周波増幅回路２７、復調回路２８によって構成され、その復調された出力信号がマイクロプロセッサ２１に入力されるように構成されている。なお、このマイクロプロセッサ２１は、予め定められた処理に基づいて、復調された出力信号から暗号化されたローリングコードを復元する。

【００２２】

マイクロプロセッサ２１には、ＥＥＰＲＯＭ２９が接続されており、このＥＥＰＲＯＭ２９には、受信機２固有のＩＤコード、送信機１から前回受信した送信コードに含まれていたローリングコード、車両固有のキーコード、及び登録用キーコードが記憶されている。なお、このＩＤコード、車両固有のキーコード、及び登録用キーコードの各コードは、送信機が記憶するＩＤコード、車両固有のキ

ーコード、及び登録用キーコードの各々と同一の内容となっている。

【００２３】

また、ＥＥＰＲＯＭ２９には、マイクロプロセッサ２１が暗号化されたローリングコードを復元する際に用いる変更テーブル（図２と同じ）が記憶されるとともに、出力信号から暗号化ローリングコードを復元するための復号化アルゴリズムがプログラムとして記憶されている。

【００２４】

さらに、マイクロプロセッサ２１には、駆動回路２３－１、２３－２、・・・、２３－ｎを介して、制御対象となる２２－１、２２－２、・・・、２２－ｎ（例えば、車両の各ドアのロック・アンロック、トランクの開閉、シートポジションの設定等を行うアクチュエータ）が接続されており、この制御対象となる２２－１、２２－２、・・・、２２－ｎは、マイクロプロセッサ２１からの信号に応じて作動するように構成されている。

【００２５】

（通常動作）

次に、上記構成の送信機１及び受信機２による、制御対象を遠隔操作する際の動作について、図４及び図５のフローチャートを用いて説明する。先ず、図４のステップＳ１では、送信機１のスイッチ１２－１、１２－２、・・・、１２－ｎのいずれかが操作されたか否かを判断する。ここで、いずれかのスイッチが操作された場合には、ステップＳ２へ処理を進め、いずれのスイッチも操作されていない場合には、操作されるまで待機状態となる。

【００２６】

ステップＳ２では、ＥＥＰＲＯＭ１３に記憶されるローリングコードの更新を行う。このローリングコードは、ｍビットからなる変数で、送信機１から送信が行われる毎に、所定の規則（例えば、シフト演算等）に従って変化する。

【００２７】

ステップＳ３では、ローリングコードを暗号化して暗号化ローリングコードを生成する。この暗号化ローリングコードの生成方法を、図２に示す変換テーブル及び図３に示す暗号化アルゴリズムを用いて説明する。

【００２８】

先ず、図３において、図２に示す１番目の共通鍵コード［ＫＥＹ（１）］とローリングコードとの排他的論理和の演算を行う。次に、排他的論理和の演算結果に対して、周知のＭ系列演算を行う。その後、２番目以降の共通鍵コードを用いた排他的論理和の演算とＭ系列演算を（ｎ－１）回繰り返す。これにより、ローリングコードが暗号化され、最終的に暗号化ローリングコードが生成される。

【００２９】

なお、ｋ回目の排他的論理和の演算では、車両固有のキーコードがｋ番目の共通鍵コード［ＫＥＹ（ｋ）］として用いている。これにより、ｋ回目の排他的論理和の演算方法は車両毎に異なることになり、さらには、暗号化の方法が車両によって異なることになる。

【００３０】

ステップＳ４では、ステップＳ３において暗号化された暗号化ローリングコード、ＥＥＰＲＯＭ１３に記憶されるＩＤコード、及び機能コードを用いて送信コードを生成する。この送信コードは、例えば、これらの各コードにフォーマットビット（スタートビット、ストップビット、パリティビット）を付加し、さらに所定ビット数からなる乱数を加えて送信コードを構成する。

【００３１】

なお、機能コードとは、制御対象となる２２－１、２２－２、・・・、２２－ｎを作動させるためのコードであり、ステップＳ１おいて操作された各機能（例えば、車両の各ドアのロック・アンロック、トランクの開閉、シートポジションの設定等）を遠隔作動させるためのスイッチ１２－１、１２－２、・・・、１２－ｎに対応したものである。

【００３２】

そして、ステップＳ５において、ステップＳ４で生成した送信コードをＦＭ変調回路１５を介して出力する。これにより、送信コードはＦＭ変調されて微弱電波として送信機１の外部に発信される。

【００３３】

続いて、受信機２が上述の送信コードを受信してから制御対象に制御指令を出

力するまでの動作について、図５のフローチャートを用いて説明する。先ず、ステップＳ１０において、送信機１からの送信コードを受信したか否かを判断する。ここで、送信コードを受信した場合には、ステップＳ１１へ処理を進め、送信コードを受信していない場合には、受信するまで待機状態となる。

【００３４】

ステップＳ１１では、送信コードから暗号化ローリングコード、ＩＤコード及び機能コードを抽出し、この抽出した暗号化ローリングコードを復元する。なお、暗号化ローリングコードの復元には復号化アルゴリズムが用いられる。そして、ステップＳ１２において、抽出したＩＤコードとＥＥＰＲＯＭ２９に記憶されているＩＤコードとが一致するか否かを判断する。ここで、ＩＤコードが一致するならば、ステップＳ１３へ処理を進め、これに該当しない場合には、ステップＳ１０へ処理を移行し、再び送信コードの受信待ちとなる。

【００３５】

ステップＳ１３では、ステップＳ１１において復元されたローリングコードと、ＥＥＰＲＯＭ２９に記憶されているローリングコードとを比較し、復元されたローリングコードが記憶されるローリングコードに対し、所定の範囲内にあるか否かを判定する。ここで、所定の範囲内にある場合には、ステップＳ１４へ処理を進め、これに該当しない場合には、ステップＳ１０へ処理を移行し、再び送信コードの受信待ちとなる。

【００３６】

なお、ステップＳ１３では、送信機１から送信される送信コードが、受信機２で毎回確実に受信できない場合を考慮している。すなわち、送信機１から送信コードが送信されても、例えば電波干渉等の理由により、受信機２で送信コードが受信できない（いわゆる送信機１のカラ打ち）場合がある。このとき、送信機１のローリングコードのみが更新されるため、このカラ打ちに対応できるように、許容範囲を定めている。

【００３７】

このように、本実施形態では、復号化されたローリングコードが、予め定められた関係を満足しているか否かを判定している。

【００３８】

ステップＳ１４では、受信機２のＥＥＰＲＯＭ２９に記憶されているローリングコードを一旦消去したのち、送信コードから復元したローリングコードを新たなローリングコードとして記憶する。以後、ステップＳ１３の処理では、この新たに記憶されたローリングコードと復元したローリングコードとを比較する。そして、ステップＳ１５において、送信コードに設定されていた機能コードを参照し、駆動回路２３－１、２３－２、・・・、２３－ｎを介して、制御対象となる２２－１、２２－２、・・・、２２－ｎを作動させる。

【００３９】

（キーコード登録）

次に、本実施形態の特徴部分である、車両固有のキーコードを送信機１から受信機２へ送信して登録する際の、送信機１及び受信機２の動作について、図８及び図９のフローチャートを用いて説明する。なお、送信機１から登録すべきキーコードを送信する前に、受信機２をキーコード登録のモードに予め変更しておく。このモード変更については、例えば、別途用意される登録専用の送信機等からモード変更の信号を受信機２に対して送信するなどして、モードを変更する。

【００４０】

さらに、受信機２のモードがキーコード登録モードに変更されたとき、キーコードを復号化するための変換テーブル（図２と同じ）のｋ番目の共通鍵コード［ＫＥＹ（ｋ）］を、ＥＥＰＲＯＭ２９に記憶される登録用のキーコードに変更する。この登録用キーコードは、ｍビットからなる変数であり、例えば、０００００やｆｆｆｆ等である。

【００４１】

先ず、ステップＳ２０は、送信機１におけるスイッチ１２－１、１２－２、・・・、１２－ｎの特定の操作がなされたか否かを判断する。ここで、特定の操作がなされた場合には、ステップＳ２１へ処理を進め、これに該当しない場合には、スイッチ操作がなされるまで待機状態となる。この特定のスイッチ操作がなされた場合に、送信機１ではキーコードを暗号化して受信機２へ送信する。従って、送信機１の登録すべきキーコードを容易に受信機２へ送信することができる。

【００４２】

なお、この特定のスイッチ操作とは、通常、ユーザが制御対象を遠隔操作するために操作するスイッチの押し方とは異なるもので、例えば、特定の複数のスイッチ１２－１、１２－２、・・・、１２－ｎを同時に押したり、複数のスイッチ１２－１、１２－２、・・・、１２－ｎを特定の順序で押したりする操作である。但し、キーコードを暗号化して送信させるための操作として、このようなスイッチ操作に限定されるものではない。

【００４３】

ステップＳ２１では、図６に示すように、ＥＥＰＲＯＭ１３に記憶される変換テーブルのうち、ｋ番目の共通鍵コード［ＫＥＹ（ｋ）］を、同じくＥＥＰＲＯＭ１３に記憶される登録用キーコードに変更する。この登録用キーコードは、上述の如く、ｍビットからなる変数であり、例えば、０００００やｆｆｆｆ等である。

【００４４】

ステップＳ２２では、ＥＥＰＲＯＭ１３に記憶される車両固有のキーコードを抽出し、これを暗号化して暗号化キーコードを生成する。この暗号化キーコードの生成方法については、上述のローリングコードを暗号化して暗号化ローリングコードを生成する方法と同一であり、図６に示す変換テーブルのｋ番目の共通鍵コードに登録用キーコードを用いた点と、図７に示すように、暗号化アルゴリズムを用いて暗号化する対象が車両固有のキーコードになる点のみ異なる。よって、暗号化キーコードの生成方法に関する説明は省略する。

【００４５】

このように、本実施形態におけるキーコードの暗号化は、制御対象を遠隔操作する際のローリングコードを暗号化する暗号化アルゴリズムを使用するため、専用の暗号化アルゴリズムを用意する必要がなく、ソフト容量の節約や管理工数が削減できる。

【００４６】

ステップＳ２３では、ステップＳ２２において暗号化された暗号化キーコード、及びＥＥＰＲＯＭ１３に記憶されるＩＤコードを用いて送信コードを生成する

。この送信コードは、上述のように、例えば、これらの各コードにフォーマットビット（スタートビット、ストップビット、パリティビット）を付加し、さらに所定ビット数からなる乱数を加えて送信コードを構成する。

【００４７】

そして、ステップＳ２４において、ステップＳ２３で生成した送信コードをＦＭ変調回路１５を介して出力する。これにより、暗号化キーコードを含む送信コードがＦＭ変調されて、微弱電波として送信機１の外部に発信される。

【００４８】

続いて、受信機２が上述の暗号化キーコードを含む送信コードを受信し、復元したキーコードを記憶するまでの動作について、図９のフローチャートを用いて説明する。先ず、ステップＳ３０において、送信機１からの送信コードを受信したか否かを判断する。ここで、送信コードを受信した場合には、ステップＳ３１へ処理を進め、送信コードを受信していない場合には、受信するまで待機状態となる。

【００４９】

ステップＳ３１では、送信コードからＩＤコード及び暗号化キーコードを抽出し、抽出した暗号化キーコードを復元する。なお、暗号化キーコードの復元は、登録用キーコードが設定された変更テーブルを用いて復元する。そして、ステップＳ３２において、抽出したＩＤコードとＥＥＰＲＯＭ２９に記憶されているＩＤコードとが一致するか否かを判断する。ここで、ＩＤコードが一致するならば、ステップＳ３３へ処理を進め、これに該当しない場合には、ステップＳ１０へ処理を移行し、再び送信コードの受信待ちとなる。

【００５０】

ステップＳ３３では、送信コードから復元したキーコードを受信機２のＥＥＰＲＯＭ２９へ記憶する。あるいは、既にキーコードがＥＥＰＲＯＭ２９に記憶されている場合には、既に記憶されているキーコードを一旦消去したのち記憶する。

【００５１】

このように、本実施形態の遠隔操作装置は、送信機１のキーコードを暗号化し

たうえで受信機２へ送信している。これにより、キーコードを送信機１から受信機２へ送信して登録する際、仮に、この送信時に暗号化されたキーコードが盗聴されたとしても、キーコード取得の困難性を向上することができる。その結果、送信機１の不正な複製を防止することが可能となる。

【００５２】

なお、本実施形態において説明した暗号化アルゴリズム及び復号化アルゴリズムは、排他的論理和の演算やＭ系列演算による暗号化に限定されるものではない。

【００５３】

また、通常動作及びキーコード登録の処理において、送信機１から送信される送信コードに含まれるＩＤコードを暗号化しても良い。そして、暗号化されたＩＤコードを含む送信コードを送信し、この送信コードを受信する受信機２において暗号化されたＩＤコードを復元しても良い。

【００５４】

（第２の実施形態）

本実施形態では、本発明の遠隔操作装置を電子キーシステムに採用した例について説明する。本実施形態の電子キーシステムは、携帯機（電子キー）側と車両側との双方向通信による車両の内外での所定コードの照合結果を基に、車両に設けられたセキュリティＥＣＵが各ドアのロック機構やステアリング機構を制御し、さらに、車両のエンジンの始動の許可・禁止状態を制御するものである。

【００５５】

図１０は、本実施形態の電子キーシステムの全体の構成を示す図である。同図に示すように、車両３２には車両側発信機３３が設けられ、セキュリティＥＣＵ３５からの指示に基づいて、所定間隔毎にチャレンジコード信号を発信する。この車両側発信機３３は、車両３２の複数箇所に設けられ、かつ、それぞれの発信機３３から発信されるチャレンジコード信号の到達距離が設定されている。従って、このチャレンジコード信号の到達距離に応じた検知エリア３１が車両３２の周囲に形成され、携帯機３０の携帯者が車両３２に接近したことを即座に検知できるようにしている。

【００５６】

携帯機３０は、車両側発信機３３からのチャレンジコード信号を受信したり、暗号化したチャレンジコードとＩＤコードとを含む送信コード信号を送信したりする送受信回路（図示せず）を備えている。また、受信したチャレンジコード信号を暗号化するマイクロプロセッサ（図示せず）と、携帯機３０固有のＩＤコード、車両固有のキーコード及び登録用キーコード（デフォルトキーコード）を記憶するＲＡＭ（図示せず）も備えている。

【００５７】

また、このＲＡＭには、チャレンジコードを暗号化する際に用いる変更テーブル（図１１）が記憶されるとともに、暗号化アルゴリズム（図１２）がプログラムとして記憶されている。従って、携帯機３０が検知エリア３１内に入ったとき、携帯機３０は、即座にチャレンジコード信号を受信し、この受信したチャレンジコードを暗号化したのち、ＩＤコードを付した送信コード信号を発信する。

【００５８】

なお、図１１に示すように、変更テーブルは、各々異なるｍビットからなるｎ個の共通鍵コード［ＫＥＹ（１）～ＫＥＹ（ｎ）］が設定されている。このうち、ｋ番目の共通鍵コードには、ＲＡＭに記憶されている車両固有のキーコードが設定されている。

【００５９】

携帯機３０から発信された送信コード信号は、車両３２に設けられたワイヤレスレシーバ３４によって受信される。この受信した送信コード信号は、セキュリティＥＣＵ３５に出力され、セキュリティＥＣＵ３５にて、暗号化されたチャレンジコードが復元される。

【００６０】

このセキュリティＥＣＵ３５は、図示しないＲＡＭを有し、このＲＡＭには、暗号化されたチャレンジコードを復元する際に用いる変更テーブル（図１１と同じ）が記憶されるとともに、暗号化されたチャレンジコードを復元するための復号化アルゴリズムがプログラムとして記憶されている。さらに、このＲＡＭには、車両固有のキーコード及び登録用キーコードが記憶されている。

【００６１】

セキュリティＥＣＵ３５は、ＩＤコード及び暗号化されたチャレンジコードを抽出し、この暗号化されたチャレンジコードを復元する。そして、ＲＡＭに記憶されているＩＤコードと抽出したＩＤコードとが一致したか否かを判定する。さらに、車両側発信機３３から発信したＲＡＭに記憶されるチャレンジコードと復元したチャレンジコードとが一致したか否かをも判定する。

【００６２】

ここで、ＩＤコード及びチャレンジコードの両方が一致したと判定されると、ドアロック機構３６やラッゲージドアロック機構３９をアンロックスタンバイ状態にする。そして、ドアハンドルに設けられたタッチスイッチ（図示しない）によって、ドアハンドルの操作の開始が検出されると、ドアやラッゲージドアをアンロック状態にする。

【００６３】

このように、本実施形態では、復元されたチャレンジコードが予め定めた関係を満足しているか否かを判定している。

【００６４】

一方、ドアを開閉して携帯機３０の携帯者が乗車すると、車室内に設けられた車両側発信機３３及びワイヤレスレシーバ３４を用いて携帯機３０との間で双方向通信を行い、再度、ＩＤコード及びチャレンジコードの照合を行う。このとき、ＩＤコードの照合結果及びチャレンジコードの照合結果が「一致」であると、ステアリンクロック機構３７をアンロックスタンバイ状態にする。この状態で、予め車両３２に設けられているエンジンスイッチ（図示せず）が操作されると、ステアリンクロック機構３７がアンロックされるとともに、エンジンＥＣＵ３８に対してエンジンの始動禁止を解除するように指示信号を出力する。

【００６５】

このようにして、携帯機３０の携帯者は、携帯機３０を手に取ることなく、ドアのアンロックによる乗車からエンジンの始動までを行うことができる。

【００６６】

また、車両３２が停車し、エンジンスイッチがオフされた後に、携帯機３０の

携帯者が降車し、ドアハンドルに設けられたドアロックスイッチを操作すると、車両３２の各ドアがロックされる。このドアロックと同時に、エンジンＥＣＵ３８によってエンジンが始動禁止状態に設定される。

【００６７】

このように、本実施形態における電子キーシステムは、携帯機３０を携帯しているのみで、ドアのロック・アンロックを含む車両３２のセキュリティの設定・解除を自動的に行うことができるものである。

【００６８】

（通常動作）

次に、上記構成の携帯機３０及び車両３２との双方向通信による、ドアロック機構３６やラッゲージロック機構３９を遠隔操作する際の動作について、図１３及び図１４のフローチャートを用いて説明する。

【００６９】

先ず、図１３に示すステップＳ４０では、携帯機３０において、車両側発信機３３から所定間隔毎に発信されるチャレンジコード信号を受信したか否かを判断する。ここで、チャレンジコード信号を受信した場合には、ステップＳ４１に処理を進め、これに該当しない場合には、チャレンジコード信号を受信するまで待機状態となる。

【００７０】

ステップＳ４１では、受信したチャレンジコード信号に基づいて、このチャレンジコードを暗号化した暗号化チャレンジコードを生成する。この暗号化チャレンジコードの生成方法を、図１１に示す変更テーブル及び図１２に示す暗号化アルゴリズムを用いて説明する。

【００７１】

先ず、図１１に示す１番目の共通鍵コード［ＫＥＹ（１）］と受信したチャレンジコードとの排他的論理和の演算を行う。次に、排他的論理和の演算結果に対して、周知のM系列演算を行う。その後、２番目以降の共通鍵コードを用いて排他的論理和の演算とM系列演算を（ｎ－１）回繰り返す。これにより、チャレンジコードが暗号化され、最終的に暗号化チャレンジコードが生成される。

【００７２】

なお、ｋ回目の排他的論理和の演算では、車両固有のキーコードが変更テーブルの共通鍵コード［ＫＥＹ（ｋ）］として用いている。これにより、ｋ回目の排他的論理和の演算方法は、車両毎に異なることになり、さらには、暗号化の方法が車両によって異なることになる。

【００７３】

ステップＳ４２では、ステップＳ４１において生成された暗号化チャレンジコード及びＲＡＭに記憶されるＩＤコードを用いて、送信コードを生成する。この送信コードは、例えば、暗号化チャレンジコード及びＩＤコードにフォーマットビット（スタートビット、ストップビット、パリティビット）を付加し、さらに所定ビット数からなる乱数を加えて送信コードを構成する。

【００７４】

そして、ステップＳ４３において、ステップＳ４２において生成した送信コードの信号（送信コード信号）を発信する。

【００７５】

次に、図１４に示すステップＳ５０では、携帯機３０からの送信コード信号を受信したか否かを判断する。ここで、送信コード信号を受信した場合には、ステップＳ５１へ処理を進め、送信コード信号を受信していない場合には、送信コード信号を受信するまで待機状態となる。

【００７６】

ステップＳ５１では、受信した送信コード信号からＩＤコード及び暗号化チャレンジコードを抽出し、この抽出した暗号化チャレンジコードを復元する。なお、暗号化チャレンジコードの復号化には、復号化アルゴリズムが用いられる。そして、ステップＳ５２において、抽出したＩＤコードとセキュリティＥＣＵ３５のＲＡＭに記憶されているＩＤコードとが一致するか否かを判別する。ここで、ＩＤコードが一致するならば、ステップＳ５３へ処理を進め、ＩＤコードが一致しない場合には、ステップＳ５０へ処理を移行し、再び送信コード信号の受信待ち状態となる。

【００７７】

ステップＳ５３では、ステップＳ５１において復元されたチャレンジコードと、車両側発信機３３から発信したＲＡＭに記憶されるチャレンジコードとが一致するか否かを判別する。そして、チャレンジコードが一致するならば、ステップＳ５４へ処理を進め、チャレンジコードが一致しない場合には、ステップＳ５０へ処理を移行し、再び送信コード信号の受信待ち状態となる。

【００７８】

そして、ステップＳ５４において、ドアロック機構３６及びラッゲージドアロック機構３９をアンロックスタンバイ状態にする。そして、図示しないが、ドアハンドルの操作の開始が検出されると、ドアやラッゲージドアをアンロック状態にする。なお、携帯機３０の携帯者が車両３２に乗車して、エンジンの始動禁止を解除する指示信号を出力するまでの動作は、上述の図１３及び図１４に示した処理と同様であるので、説明を省略する。

【００７９】

（キーコード登録）

次に、本実施形態の特徴部分である、携帯機３０の車両固有のキーコードを車両３２のセキュリティＥＣＵ３５へ登録する際の動作について、図１７及び図１８のフローチャートを用いて説明する。

【００８０】

なお、携帯機３０から送信コード信号を送信する前に、セキュリティＥＣＵ３５をキーコード登録のモードに変更しておく。また、このとき、セキュリティＥＣＵ３５のＲＡＭが記憶する、キーコードを復号化するための変換テーブル（図１１と同じ）のｋ番目の共通鍵コード［ＫＥＹ（ｋ）］を、登録用のキーコードに変更しておく。この登録用キーコードは、上述の如く、ｍビットからなる変数であり、例えば、０００００やｆｆｆｆ等の変数である。

【００８１】

このモード変更については、例えば、別途用意される登録専用の携帯機等からモード変更の信号を発信し、ワイヤレスレシーバ３４がこれを受信してセキュリティＥＣＵ３５のモードを変更する。また、このモード変更がなされた場合には、セキュリティＥＣＵ３５はチャレンジコードを出力しないようにする。

【００８２】

先ず、ステップＳ６０は、携帯機３０の押しボタンスイッチ（図示せず）によって、特定の操作がなされたか否かを判断する。ここで、特定の操作がなされた場合には、ステップＳ６１へ処理を進め、これに該当しない場合には、スイッチ操作がなされるまで待機状態となる。この特定のスイッチがなされた場合に、携帯機３０では、車両固有のキーコードを暗号化して送信するようになっているため、キーコードを容易に送信できる。

【００８３】

なお、この特定のスイッチ操作とは、例えば、特定の複数のスイッチを同時に押したり、複数のスイッチを特定の順序で押したりする操作である。

【００８４】

ステップＳ６１では、図１５に示すように、携帯機３０のＲＡＭに記憶される、キーコードを暗号化するための変換テーブルのｋ番目の共通鍵コード［ＫＥＹ（ｋ）］を、同じくＲＡＭに記憶される登録用のキーコードに変更する。この登録用キーコードは、ｍビットからなる変数であり、例えば、０００００やｆｆｆｆ等の変数である。

【００８５】

ステップＳ６２では、ＲＡＭに記憶される車両固有のキーコードを暗号化して暗号化キーコードを生成する。この暗号化キーコードの生成方法については、上述のチャレンジコードを暗号化して暗号化チャレンジコードを生成する方法と同一であり、図１５に示す変換テーブルのｋ番目の共通鍵コードに登録用キーコードを用いた点と、図１６に示すように、暗号化アルゴリズムを用いて暗号化する対象が車両固有のキーコードになる点のみ異なる。従って、暗号化キーコードの生成方法に関する説明は省略する。

【００８６】

このように、本実施形態におけるキーコードの暗号化は、携帯機３０から発信されたチャレンジコード信号を暗号化する際の暗号化アルゴリズムを使用するため、専用の暗号化アルゴリズムを用意する必要がなく、ソフト容量の節約や管理工数が削減できる。

【００８７】

ステップＳ６３では、ステップＳ６２において暗号化された暗号化キーコード、及びＲＡＭに記憶されるＩＤコードを用いて送信コードを生成する。この送信コードは、上述のように、例えば、これらの各コードにフォーマットビット（スタートビット、ストップビット、パリティビット）を付加し、さらに所定ビット数からなる乱数を加えて送信コードを構成する。そして、ステップＳ６４において、ステップＳ６３で生成した送信コードを発信する。

【００８８】

続いて、ワイヤレスレシーバ３４が、上述の暗号化キーコードを含む送信コードを受信してから、復元したキーコードを記憶するまでの動作について、図１８のフローチャートを用いて説明する。

【００８９】

先ず、ステップＳ７０において、携帯機３０からの送信コードをワイヤレスレシーバ３４が受信したか否かを判断する。ここで、送信コードを受信した場合には、ステップＳ７１へ処理を進め、送信コードを受信していない場合には、受信するまで待機状態となる。

【００９０】

ステップＳ７１では、送信コードからＩＤコード及び暗号化キーコードを抽出し、この抽出した暗号化キーコードを復元する。なお、暗号化キーコードの復元は、登録用キーコードが設定された変更テーブルを用いて復元する。そして、ステップＳ７２において、抽出したＩＤコードとセキュリティＥＣＵ３５のＲＡＭに記憶されているＩＤコードとが一致するか否かを判断する。ここで、ＩＤコードが一致するならば、ステップＳ７３へ処理を進め、これに該当しない場合には、ステップＳ１０へ処理を移行し、再び送信コードの受信待ちとなる。

【００９１】

ステップＳ７３では、セキュリティＥＣＵ３５のＲＡＭへ、送信コードから復元したキーコードを記憶する。あるいは、既にキーコードが記憶されている場合には、既に記憶されているキーコードを復元したキーコードに上書き記憶する。

【００９２】

このように、携帯機と車両との双方向通信によって、車両の各ドアのロック機構やステアリングロック機構を制御したり、車両のエンジンの始動の許可・禁止状態を制御したりする電子キーシステムに、本実施形態の遠隔操作装置を適用することによって、固有キーコードの解読を容易にすることを防止できる。その結果、携帯機の不正な複製を防止することが可能となる。

【００９３】

なお、本実施形態において説明した暗号化アルゴリズム及び復号化アルゴリズムは、排他的論理和の演算やＭ系列演算による暗号化に限定されるものではない。

【００９４】

また、通常動作及びキーコード登録の処理において、携帯機３０から発信される送信コードに含まれるＩＤコードを暗号化しても良い。そして、携帯機３０から暗号化されたＩＤコードを含む送信コードを発信し、この送信コードを受信する車両３２のセキュリティＥＣＵ３５において暗号化されたＩＤコードを復元しても良い。

【図面の簡単な説明】

【図１】第１の実施形態に係わる、送信機１及び受信機２の構成を示すブロック図である。

【図２】第１の実施形態に係わる、ローリングコードを暗号化するための変更テーブルを示す図である。

【図３】第１の実施形態に係わる、暗号化アルゴリズムを示す図である。

【図４】第１の実施形態に係わる、制御対象を遠隔操作する際の送信機１の処理を示すフローチャートである。

【図５】第１の実施形態に係わる、制御対象を遠隔操作する際の受信機２の処理を示すフローチャートである。

【図６】第１の実施形態に係わる、キーコード登録の際に用いる、キーコードを暗号化するための変更テーブルを示す図である。

【図７】第１の実施形態に係わる、キーコードを暗号化する暗号化アルゴリズムを示す図である。

【図８】第１の実施形態の係わる、キーコードを送信する際の送信機１の処理を示すフローチャートである。

【図９】第１の実施形態に係わる、キーコードを登録する際の受信機２の処理を示すフローチャートである。

【図１０】第２の実施形態に係わる、電子キーシステムの全体の構成を示す図である。

【図１１】第２の実施形態に係わる、チャレンジコードを暗号化するための変更テーブルを示す図である。

【図１２】第２の実施形態に係わる、暗号化アルゴリズムを示す図である。

【図１３】第２の実施形態に係わる、携帯機３０の通常動作における処理を示すフローチャートである。

【図１４】第２の実施形態に係わる、車両３２側の通常動作における処理を示すフローチャートである。

【図１５】第２の実施形態に係わる、キーコード登録の際に用いる、キーコードを暗号化するための変更テーブルを示す図である。

【図１６】第２の実施形態に係わる、キーコードを暗号化する暗号化アルゴリズムを示す図である。

【図１７】第２の実施形態に係わる、キーコード登録の際の携帯機３０における処理を示すフローチャートである。

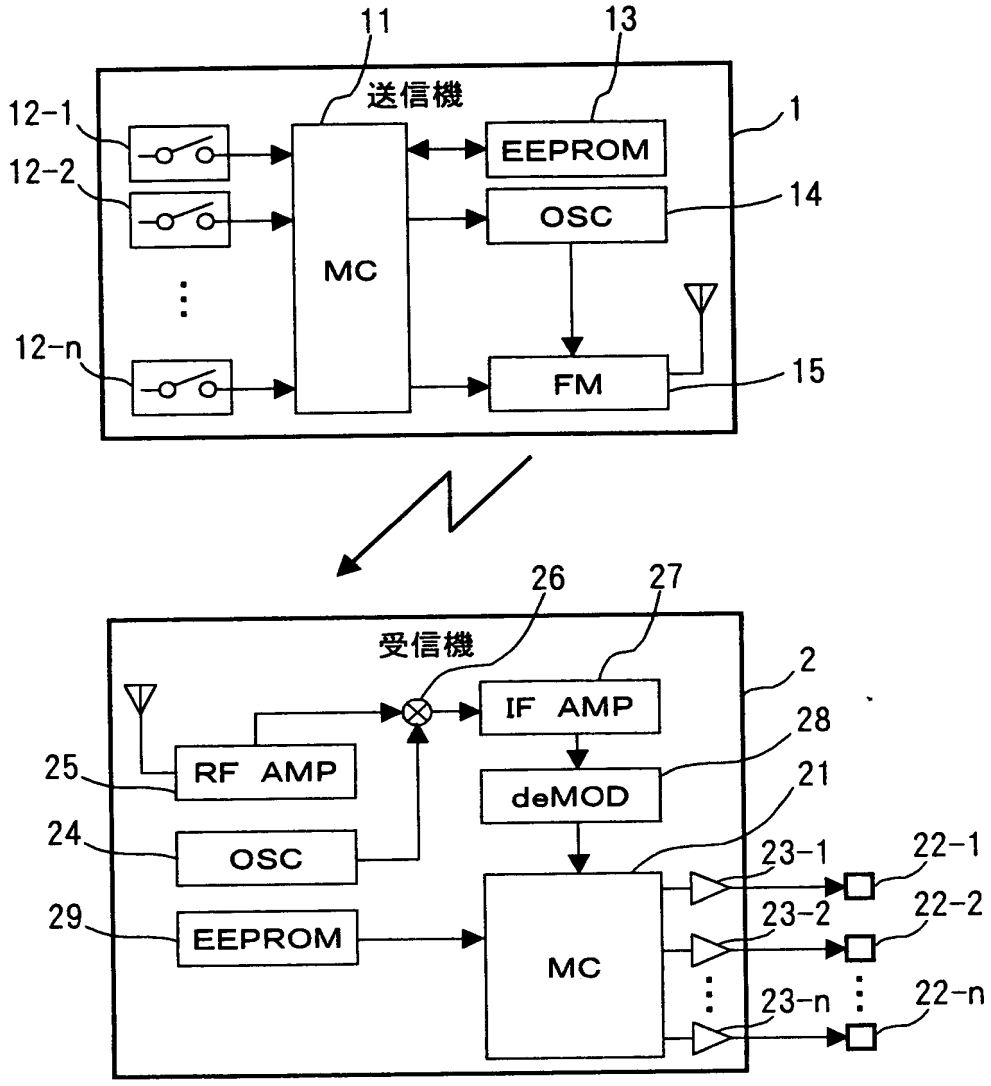
【図１８】第２の実施形態に係わる、キーコード登録の際の車両３２における処理を示すフローチャートである。

【符号の説明】

１･･･送信機、２･･･受信機、３０･･･携帯機、３２･･･車両、３５･･･セキュリティＥＣＵ

【書類名】　　図面

【図１】


11
13
送信機
12-1
12-2
12-n
MC
EEPROM
OSC
FM
1
14
15
26
27
受信機
2
IF AMP
28
deMOD
21
25
RF AMP
24
OSC
29
EEPROM
MC
23-1
23-2
23-n
22-1
22-2
22-n

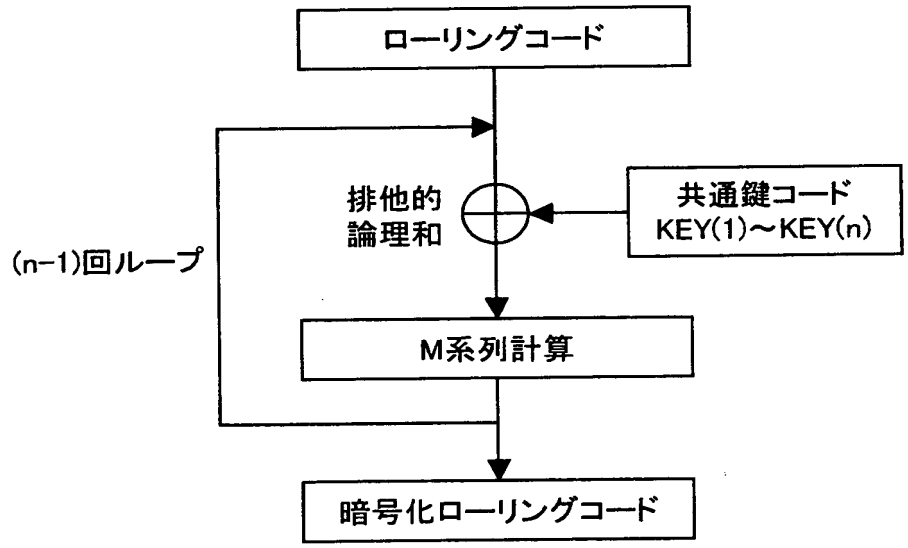
【図２】

変更テーブル

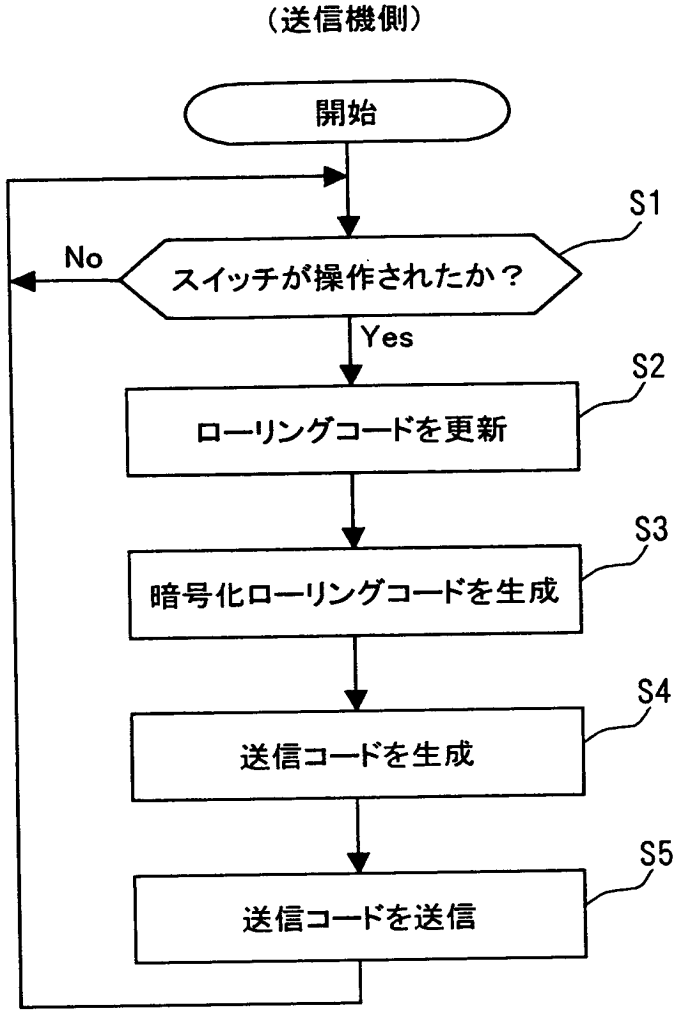
No.	共通鍵コード（mビット）
1	KEY(1)
2	KEY(2)
・ ・ ・	・ ・ ・
k	KEY(k)
・ ・ ・	・ ・ ・
n	KEY(n)

車両固有の
キーコード

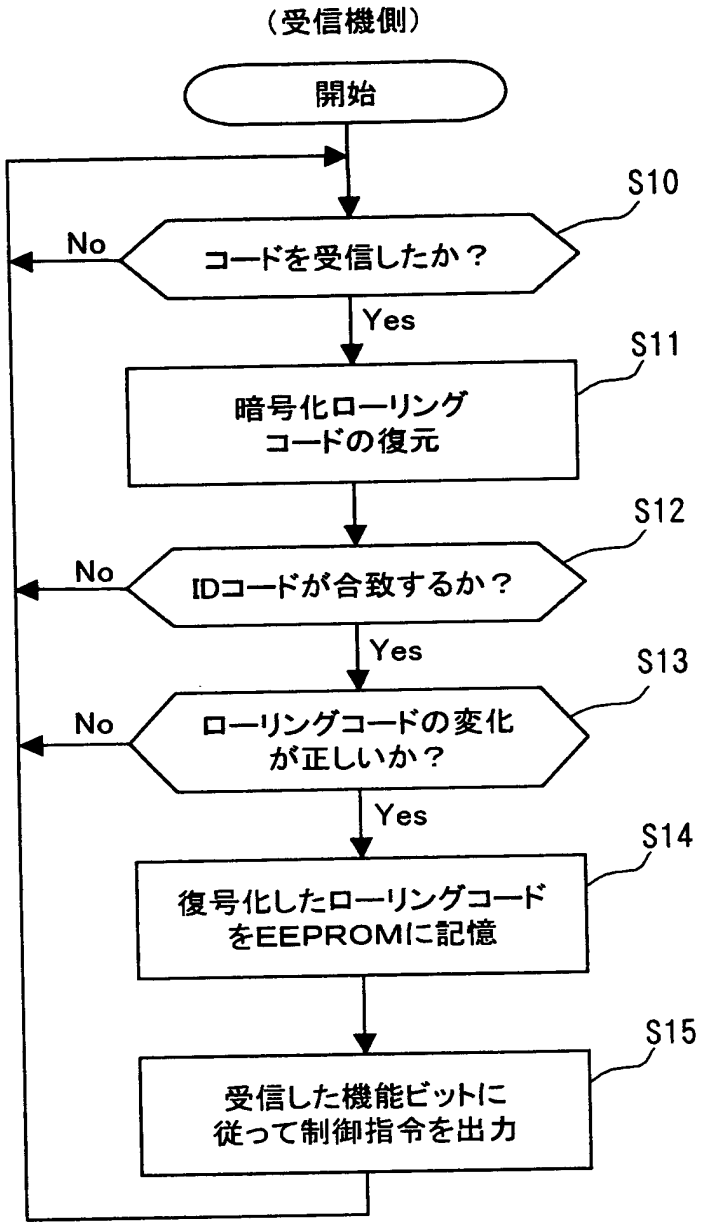
【図３】



【図４】


（送信機側）
開始
S1
No
スイッチが操作されたか？
Yes
S2
ローリングコードを更新
S3
暗号化ローリングコードを生成
S4
送信コードを生成
S5
送信コードを送信

【図５】


（受信機側）
開始
S10
No
コードを受信したか？
Yes
S11
暗号化ローリング
コードの復元
S12
No
IDコードが合致するか？
Yes
S13
No
ローリングコードの変化
が正しいか？
Yes
S14
復号化したローリングコード
をEEPROMに記憶
S15
受信した機能ビットに
従って制御指令を出力

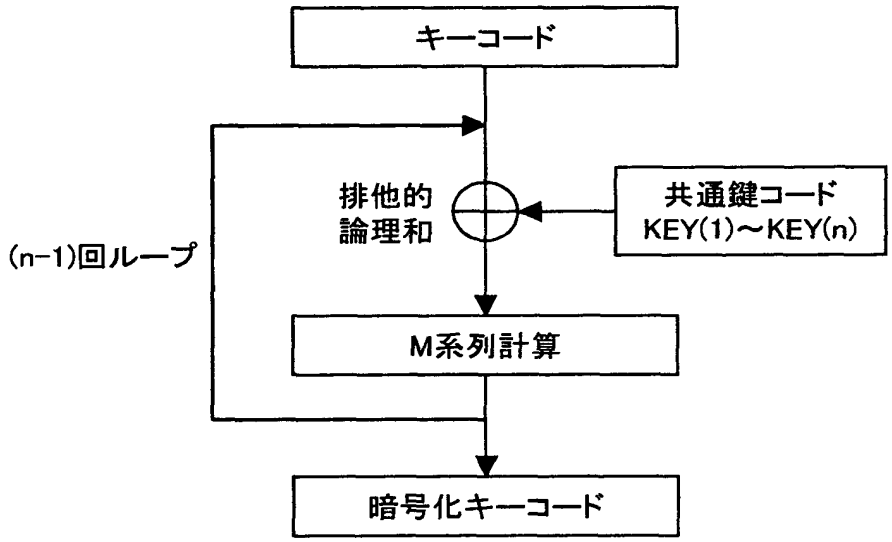
【図６】

変更テーブル

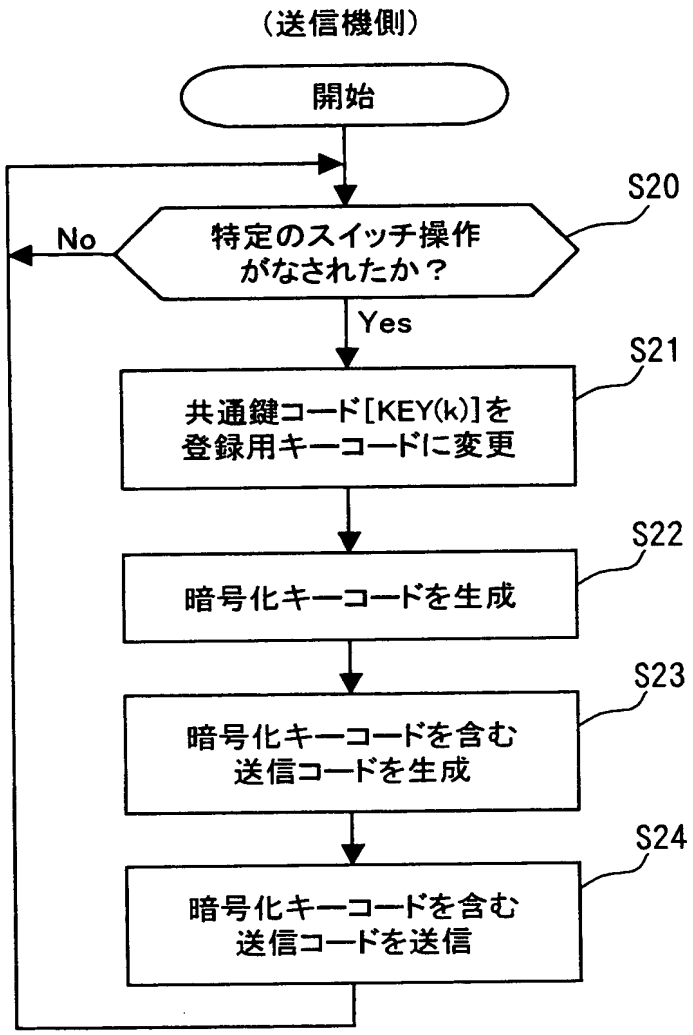
No.	共通鍵コード（mビット）
1	KEY(1)
2	KEY(2)
・ ・ ・	・ ・ ・
k	KEY(k)
・ ・ ・	・ ・ ・
n	KEY(n)

登録用キーコードに変更

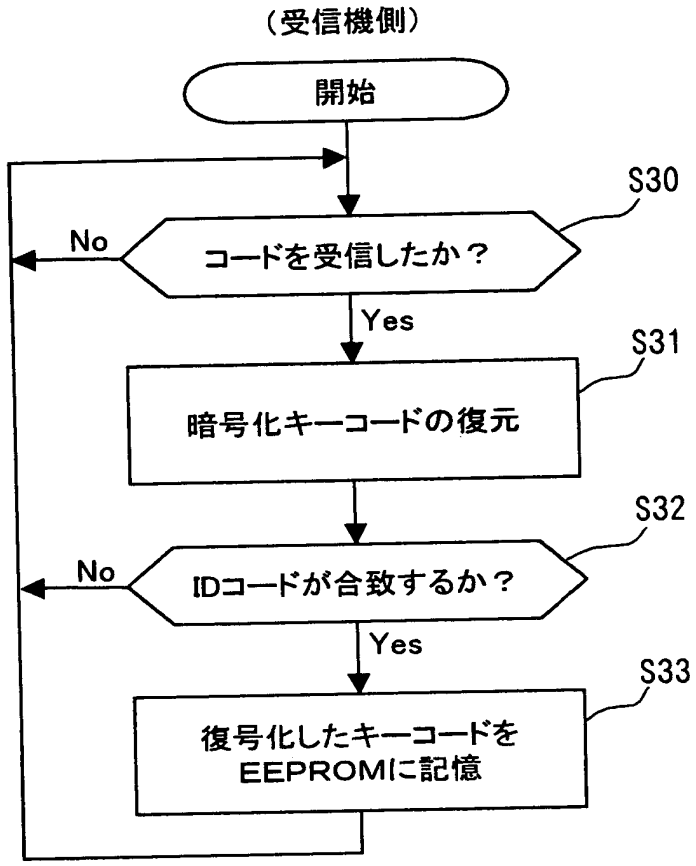
【図７】



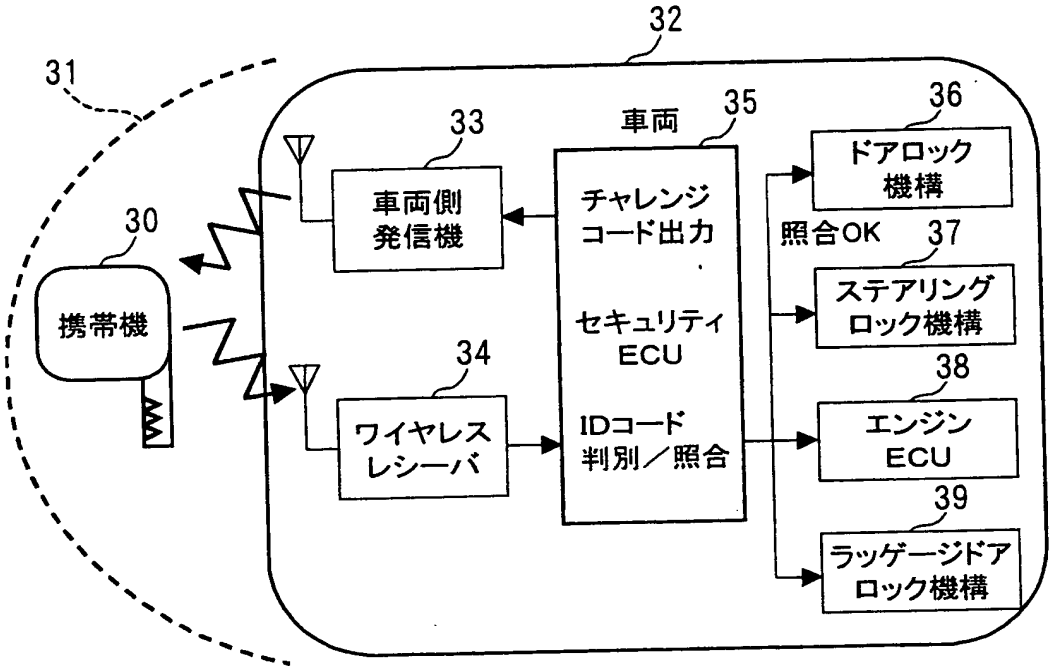
【図８】


（送信機側）
開始
S20
No
特定のスイッチ操作
がなされたか？
Yes
S21
共通鍵コード[KEY(k)]を
登録用キーコードに変更
S22
暗号化キーコードを生成
S23
暗号化キーコードを含む
送信コードを生成
S24
暗号化キーコードを含む
送信コードを送信

【図９】


（受信機側）
開始
S30
No
コードを受信したか？
Yes
S31
暗号化キーコードの復元
S32
No
IDコードが合致するか？
Yes
S33
復号化したキーコードを
EEPROMに記憶

【図１０】



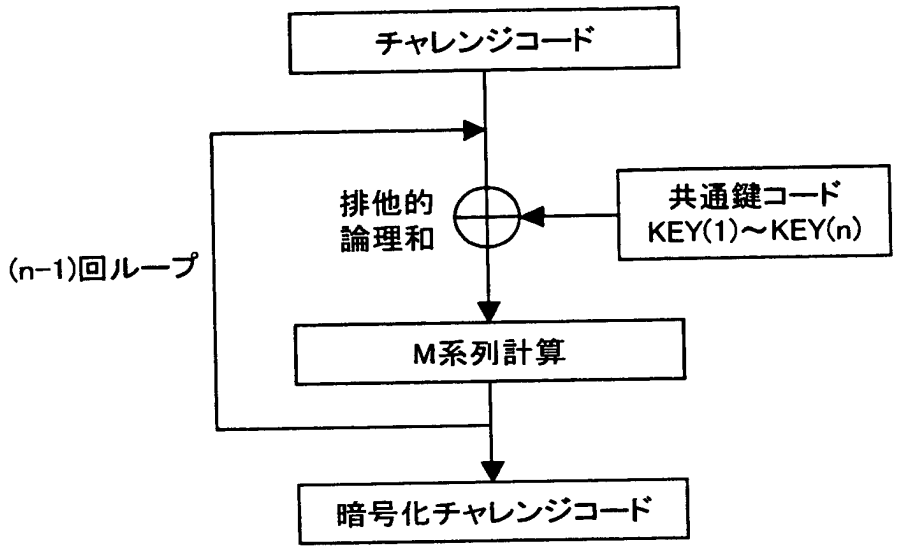
【図１１】

変更テーブル

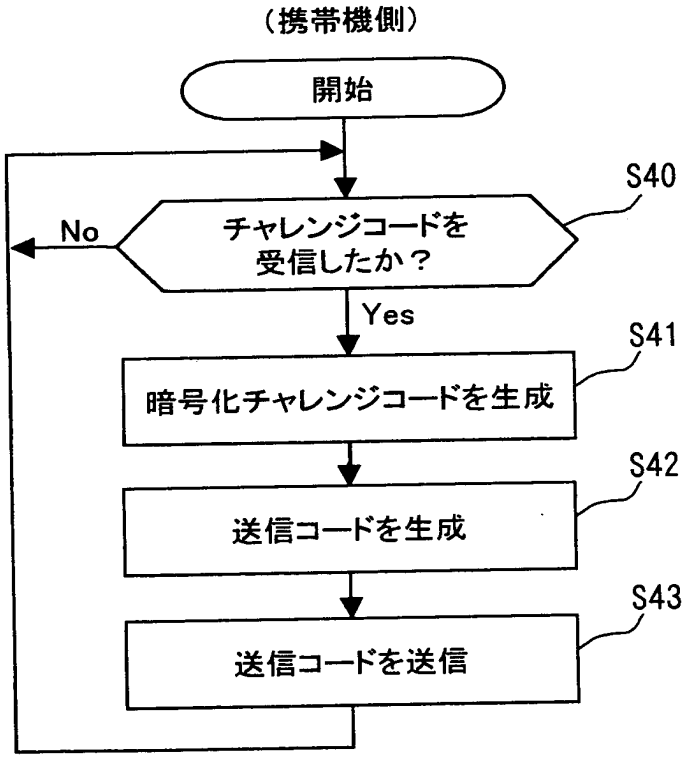
No.	共通鍵コード（mビット）
1	KEY(1)
2	KEY(2)
・ ・ ・	・ ・ ・
k	KEY(k)
・ ・ ・	・ ・ ・
n	KEY(n)

車両固有の
キーコード

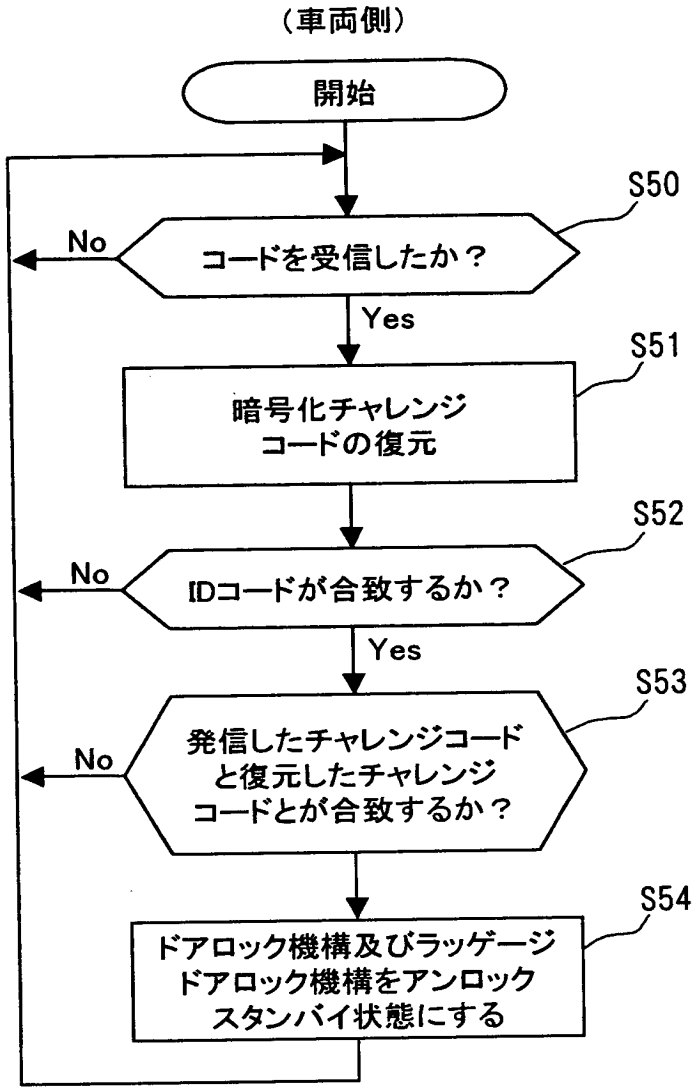
【図１２】


チャレンジコード
排他的
論理和
共通鍵コード
KEY(1)～KEY(n)
(n-1)回ループ
M系列計算
暗号化チャレンジコード

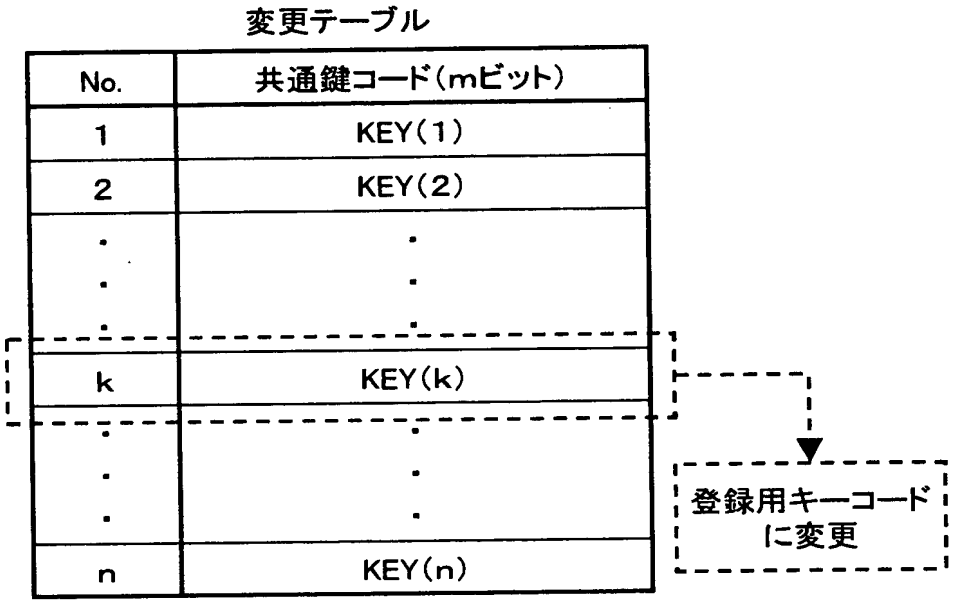
【図１３】


(携帯機側)
開始
S40
No
チャレンジコードを
受信したか？
Yes
S41
暗号化チャレンジコードを生成
S42
送信コードを生成
S43
送信コードを送信

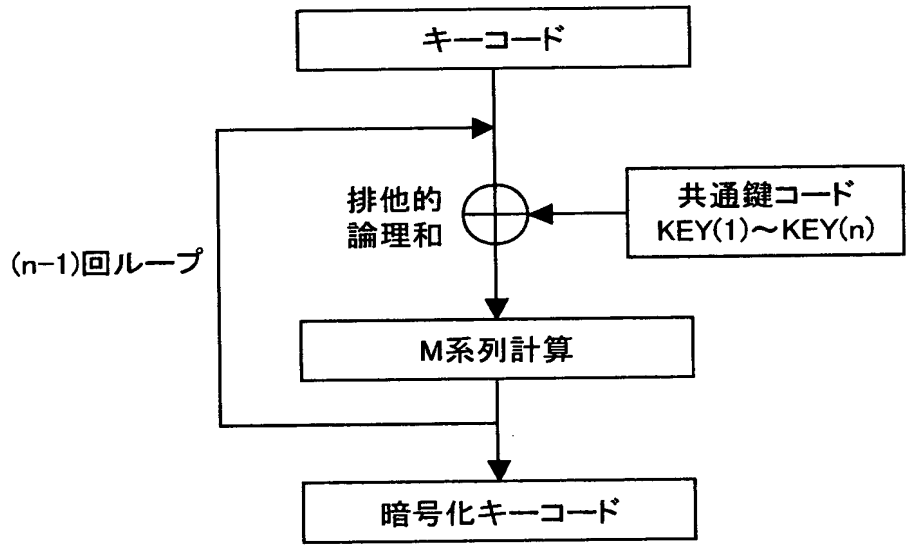
【図１４】


（車両側）
開始
S50
No
コードを受信したか？
Yes
S51
暗号化チャレンジ
コードの復元
S52
No
IDコードが合致するか？
Yes
S53
No
発信したチャレンジコード
と復元したチャレンジ
コードとが合致するか？
S54
ドアロック機構及びラッゲージ
ドアロック機構をアンロック
スタンバイ状態にする

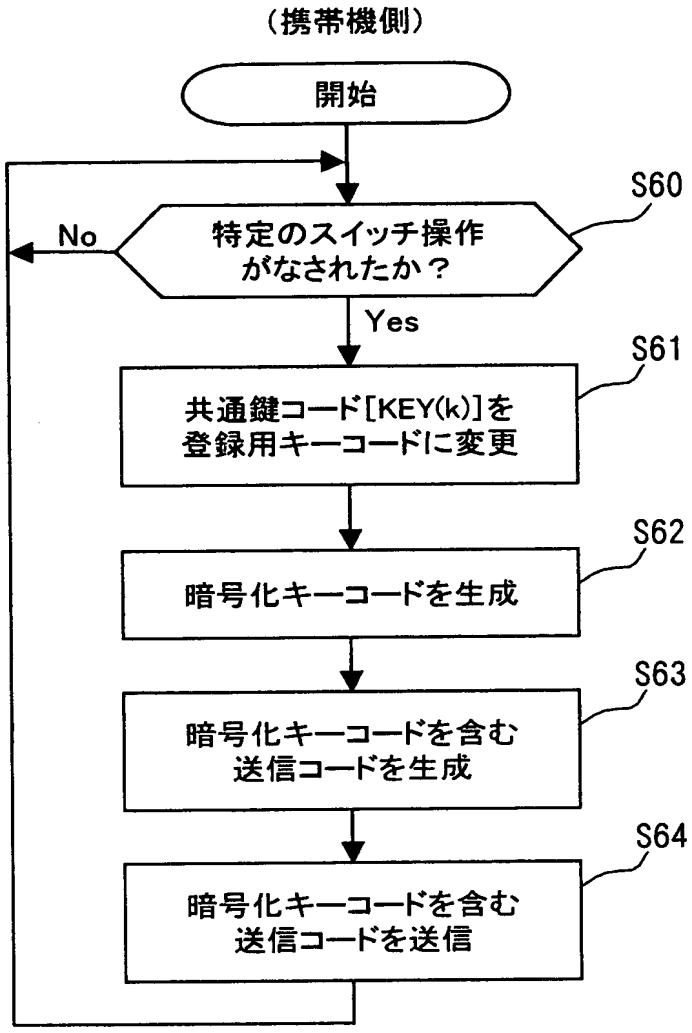
【図１５】


変更テーブル
No.
共通鍵コード(mビット)
1
KEY(1)
2
KEY(2)
k
KEY(k)
n
KEY(n)
登録用キーコード
に変更

【図１６】

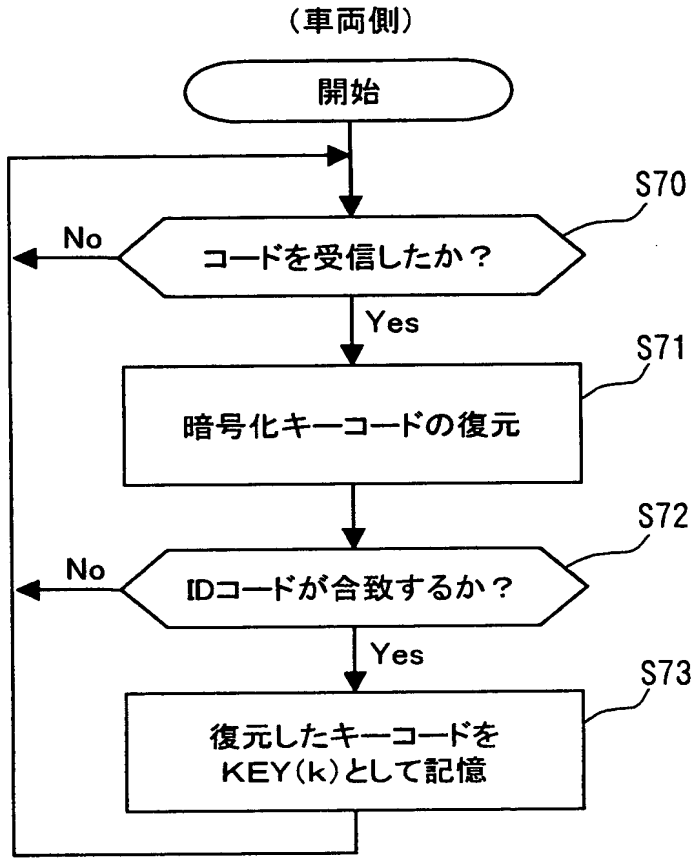

キーコード
排他的
論理和
共通鍵コード
KEY(1)～KEY(n)
(n-1)回ループ
M系列計算
暗号化キーコード

【図１７】



出証特２００３－３０５３２４４

【図１８】


（車両側）
開始
S70
No
コードを受信したか？
Yes
S71
暗号化キーコードの復元
S72
No
IDコードが合致するか？
Yes
S73
復元したキーコードを
KEY(k)として記憶

【書類名】　　要約書

【要約】

【課題】　送信機から受信機へキーコードを送信して登録するときのキーコードの解読を防止する。

【解決手段】　送信機において、特定のスイッチ操作がなされた場合に、キーコードを暗号化する変換テーブルに用いる共通鍵コードのｋ番目を、予め記憶している登録用キーコードに変更し（ステップＳ２１）、この登録用キーコードを含む変換テーブルを用いてキーコードを暗号する（ステップＳ２２）。そして、暗号化されたキーコードに、所定のコードを付して送信コードを生成し（ステップＳ２３）、この送信コードの信号を受信機へ送信する（ステップＳ２４）。これにより、送信機から受信機に送信コードを送信しているときに、例え送信コードが盗聴されたとしても、キーコードは暗号化されて送信しているため、キーコードが容易に解読されることがなくなる。

【選択図】　　図８

出　願　人　履　歴　情　報

識別番号　　〔０００００４２６０〕

１．変更年月日　　１９９６年１０月　８日
［変更理由］　名称変更
住　所　　愛知県刈谷市昭和町１丁目１番地
氏　名　　株式会社デンソー